ACTA ARITHMETICA
LXXXVIII.2 (1999)

The number of solutions of the Mordell equation

by

DIMITRIOS POULAKIS (Thessaloniki)

To the memory of André Néron

1. Introduction. Let a, b be integers such that the polynomial $f(x) = x^3 + ax + b$ has discriminant $\Delta(f) \neq 0$. In [3] Evertse and Silverman proved that the number $Z(f)$ of integer solutions of the equation $y^2 = f(x)$ satisfies

$$Z(f) \leq 7^{[L:\mathbb{Q}](4+9s)} h_2(L)^2 + 3,$$

where s is the cardinality of the set containing the usual absolute value of $\mathbb{Q}$ and the p-adic absolute values $|\cdot|_p$ for which $|\Delta(f)|_p \neq 1$, L the splitting field of $f(x)$ and $h_2(L)$ the order of the subgroup of the ideal class group of L consisting of the ideal classes $[A]$ with $[A]^2 = 1$. Using this result Schmidt [7] proved that given $\varepsilon > 0$ there is a constant $c(\varepsilon)$ depending on ε such that

$$Z(f) \leq c(\varepsilon)|\Delta(f)|^{1/2+\varepsilon}.$$

In the case of the Mordell equation (i.e. $a = 0$), it follows that $Z(f) \leq c(\varepsilon)|b|^{1+\varepsilon}$. Moreover, Schmidt conjectured that the number of solutions $x, y \in \mathbb{Z}$ of an irreducible equation $F(x, y) = 0$ defining a curve of positive genus having coefficients in $\mathbb{Z}$ and total degree N is at most

$$c(N, \varepsilon)H(F)^\varepsilon,$$

where $c(N, \varepsilon)$ is a constant depending on N and ε.

In this paper we improve on the estimate of Schmidt for the Mordell equations by showing that the number of integer solutions of $y^2 = x^3 + b$ depends only on the prime divisors of b. More precisely, we prove the following result:

THEOREM 1. *Let k be a nonzero rational integer. Denote by $\omega(k)$ the number of prime divisors of k and by $P(k)$ the product of all the prime divisors p of k with $p > 3$. If k has no prime divisors > 3, put $P(k) = 1$.*

1991 *Mathematics Subject Classification*: 11D25, 11G05.

Then the number of solutions $(x, y) \in \mathbb{Z}^2$ *of the equation* $y^2 = x^3 + k$ *is*

$$< 10^{11\omega(k)+48} P(k).$$

COROLLARY 1. *Let* k *be a nonzero rational integer and* $\Pi(k)$ *be the product of the prime divisors of* k. *Then for every* $\varepsilon > 0$ *there is a constant* $\Omega(\varepsilon)$, *independent of* k, *such that the number of solutions* $(x, y) \in \mathbb{Z}^2$ *of the equation* $y^2 = x^3 + k$ *is*

$$< \Omega(\varepsilon)\Pi(k)^{1+\varepsilon}.$$

The above theorem is a consequence of the following effective version of Shafarevich's theorem ([5, p. 222], [8, p. 263]):

THEOREM 2. *Let* S *be a finite set of rational primes with* $2, 3 \in S$. *Denote by* $P(S)$ *the product of all the primes* p *in* S *with* $p > 3$. *If* $S = \{2, 3\}$, *put* $P(S) = 1$. *Then the number of* $\mathbb{Q}$*-isomorphism classes of elliptic curves over* $\mathbb{Q}$ *with good reduction outside* S *is*

$$< 10^{11\sharp S+26} P(S).$$

In [1] there is an effective proof of Shafarevich's theorem using the estimate of [3]. Our approach is completely different and has the advantage that does not use the results of [3]. The only Diophantine approximation result we use is the estimate for the number of solutions of the S-units equation $x + y = 1$ due to Evertse [2].

2. Auxiliary results. In this section we give some lemmas which will be useful for the proof of our results.

LEMMA 1. *Let* S *be a finite set of rational primes with* $2 \in S$ *and* $f(x) = x^3 + Ax + B$ *be a polynomial of* $\mathbb{Z}[x]$ *with distinct roots. Suppose that the elliptic curve* $E : y^2 = f(x)$ *has good reduction outside* S. *Let* $L = \mathbb{Q}(\theta)$, *where* θ *is a root of* $f(x)$. *Suppose that* $L \neq \mathbb{Q}$. *Then the discriminant* D_L *of* L *has the form*

$$D_L = \pm 2^\alpha 3^\beta \prod_p p^{s_p},$$

where the product is taken over all the primes $p \geq 5$, *with* $s_p = 0$ *for* p *outside* S *and* $0 \leq s_p \leq \deg L - 1$ *for* $p \in S$. *Moreover*, $\alpha = 0, 2, 3$ *and* $\beta \leq 1$ *if* $\deg L = 2$, *while* $\beta = 0, 1, 3, 4, 5$ *if* $\deg L = 3$.

Proof. The nonzero points of 2-torsion of E are the points $(0, \theta_i)$ $(i = 1, 2, 3)$ where θ_1, θ_2, θ_3 are the roots of $f(x)$. By [5, Theorem 1, p. 113], the extension $\mathbb{Q}(\theta_1, \theta_2, \theta_3)/\mathbb{Q}$ is unramified outside S. Then the extension $L/\mathbb{Q}$ is unramified outside S, whence the prime divisors of D_L are primes in S. Hence,

$$D_L = \pm 2^\alpha 3^\beta \prod_p p^{s_p},$$

where the product is taken over all the primes $p \geq 5$, with $s_p = 0$ for p outside S. If L is a quadratic extension, then $\alpha = 0, 2$ or 3, $\beta \leq 1$ and $s_p \leq 1$ for $p \in S$. If L is a cubic extension, [6, Theorem 2] implies that $\alpha = 0, 2$ or 3, $\beta = 0, 1, 3, 4$ or 5 and $s_p \leq 2$ for $p \in S$.

LEMMA 2. *Let D be an integer. Then the number of cubic fields of discriminant D is at most* $546|D|^{1/2}$.

Proof. Let K be a cubic field of discriminant D. Then [4, pp. 620–625] implies that $|D| \geq 23$. Let $\sigma_1, \sigma_2, \sigma_3$ be the embeddings of K into the field $\mathbb{C}$ of complex numbers. We denote by s and $2t$ the number of real and complex embeddings respectively. If $s = t = 1$, let σ_2, σ_3 be the complex embeddings. As usual denote complex conjugation by bars and define $\overline{\sigma}_i(x) = \overline{\sigma_i(x)}$. Thus $\sigma_3 = \overline{\sigma}_2$. The map $\sigma : K \to \mathbb{R}^s \times \mathbb{C}^t$ given by $\sigma(x) = (\sigma_1(x), \ldots, \sigma_{3-t}(x))$ defines an embedding of K into $\mathbb{R}^s \times \mathbb{C}^t$. The image $\sigma(O_K)$ of the ring O_K of algebraic integers of K is a lattice in $\mathbb{R}^s \times \mathbb{C}^t$. In [4, Chapter 28, §1] a structure of Euclidean space is defined on $\mathbb{R}^s \times \mathbb{C}^t$. The fundamental parallelotope of the lattice $\sigma(O_K)$ has content $|D|^{1/2}$ with respect to this Euclidean metric [4, p. 538].

Let A be the convex region in $\mathbb{R}^s \times \mathbb{C}^t$ determined by the inequalities

$$|x| + |y| + |z| \leq \varrho, \qquad |x + y + z| \leq \varrho' < \varrho \quad \text{if } (s, t) = (3, 0)$$

and

$$|x| + |y| + |\overline{y}| \leq \varrho, \qquad |x + y + \overline{y}| \leq \varrho' < \varrho \quad \text{if } (s, t) = (1, 1).$$

By [4, p. 623], the content of the region A is

$$\geq \frac{4}{3}\left(\frac{\pi}{4}\right)^t \varrho' \varrho^2.$$

We choose ϱ so that

$$\frac{4}{3}\left(\frac{\pi}{4}\right)^t \varrho' \varrho^2 \geq 8|D|^{1/2}.$$

Putting $\varrho' = \varrho/2$, we can take $\varrho = (4/\pi)^{t/3} 12^{1/3} |D|^{1/6}$. Hence, Minkowski's lattice point theorem [5, p. 601] implies that there exists an algebraic integer ξ of K satisfying

$$|\xi_1| + |\xi_2| + |\xi_3| \leq \left(\frac{4}{\pi}\right)^{t/3} 12^{1/3} |D|^{1/6}, \qquad |\xi_1 + \xi_2 + \xi_3| \leq \frac{1}{2}\left(\frac{4}{\pi}\right)^{t/3} 12^{1/3} |D|^{1/6},$$

where ξ_1, ξ_2, ξ_3 are the conjugates of ξ.

The arithmetic-geometric inequality implies

$$|\xi_1 \xi_2 \xi_3| < |D|^{1/2}.$$

For arbitrary real numbers a, b, c we have the inequality

$$ab + bc + ac \leq \tfrac{1}{2}(a + b + c)^2.$$

Hence

$$|\xi_1\xi_2+\xi_2\xi_3+\xi_1\xi_3|<2|D|^{1/3}.$$

Let $f(x)=x^3+Ax^2+Bx+C$ be the irreducible polynomial of ξ. Then

$$|A|<2|D|^{1/6}, \quad |B|<2|D|^{1/3}, \quad |C|<|D|^{1/2}.$$

The discriminant of $f(x)$ is

$$\Delta=-4A^3C+A^2B^2+18ABC-4B^3-27C^2.$$

Thus, the inequalities for A, B, C give $|\Delta|<179|D|$. We denote by $i(\xi)$ the index of ξ. We have $\Delta=i(\xi)^2D$, whence $|i(\xi)|\le 13$.

We now consider the surface given by the equation

$$F(X,Y,Z)=-4X^3Z+X^2Y^2+18XYZ-4Y^3-27Z^2-DL^2=0,$$

where L is a positive integer with $L\le 13$. The number of triples $(u,v,w)\in\mathbb{Z}^3$ with $|u|<2|D|^{1/6}$, $|v|<2|D|^{1/3}$ and $|w|<|D|^{1/2}$ satisfying $F(u,v,w)=0$ is less than $2(4|D|^{1/6}+1)(4|D|^{1/3}+1)<42|D|^{1/2}$ (we have used the fact that $|D|\ge 23$). Since we have at most 13 choices for L, the lemma follows.

LEMMA 3. *Let K be an algebraic number field of degree d and S be a finite set of places on K containing all the infinite places of K. Then the equation $x+y=1$ has at most*

$$3\cdot 7^{d+2\sharp S}$$

solutions in S-units x, y of K.

Proof. See [2].

LEMMA 4. *Let K be an algebraic number field and L be a Galois extension of K of degree l. Then each L-isomorphism class of elliptic curves defined over K splits into at most 6^l K-isomorphism classes.*

Proof. Let E and A be two elliptic curves defined over K and let $\alpha: E\to A$ be an isomorphism over L. Then we have a map $F(\alpha):\mathrm{Gal}(L/K)\to\mathrm{Aut}(E)$ defined by

$$F(\alpha)(\sigma)=\alpha^{-1}\circ\alpha^{\sigma} \quad \text{for every } \sigma\in\mathrm{Gal}(L/K).$$

Suppose now that B is another elliptic curve defined over K and $\beta: E\to B$ an L-isomorphism with $F(\alpha)=F(\beta)$. It follows that

$$\alpha^{-1}\circ\alpha^{\sigma}=\beta^{-1}\circ\beta^{\sigma} \quad \text{for every } \sigma\in\mathrm{Gal}(L/K).$$

Setting $\lambda=\beta\circ\alpha^{-1}$, we have $\lambda^{\sigma}=\lambda$ for every $\sigma\in\mathrm{Gal}(L/K)$. So, the isomorphism λ is defined over K, whence A and B are K-isomorphic. Thus, given an L-isomorphism class C of elliptic curves defined over K, the map $\alpha\to F(\alpha)$ defines an injection from the set of pairwise distinct K-isomorphism classes belonging to C into the set of maps from $\mathrm{Gal}(L/K)$

to $\mathrm{Aut}(E)$. Since the cardinality of $\mathrm{Gal}(L/K)$ is l and that of $\mathrm{Aut}(E)$ is at most 6, the lemma follows.

3. Proof of Theorem 2. Let $E : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$, be an elliptic curve having good reduction outside S. We denote by L the field obtained by adjoining to $\mathbb{Q}$ the points of order 2 of E. It is the field generated over $\mathbb{Q}$ by the roots of $x^3 + Ax + B$. We have the following cases.

1. $L = \mathbb{Q}$. Then E is isomorphic over $\mathbb{Q}$ to an elliptic curve in Legendre form

$$E_\lambda : \quad y^2 = x(x-1)(x-\lambda),$$

where $\lambda \in \mathbb{Q}$. The j-invariant of E_λ is

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Since E has good reduction outside S, j is a S-integer of $\mathbb{Q}$. Let $|\cdot|_p$ be a p-adic absolute value with p outside S. If $|\lambda|_p \neq 1$, then $|j|_p > 1$ from the equation for j, contradicting the fact that j is a S-integer. It follows that λ is a S-unit. Similarly for $1 - \lambda$. Thus, λ and $\mu = 1 - \lambda$ are two S-units satisfying $\lambda + \mu = 1$. By Lemma 3, the number of S-units x, y of $\mathbb{Q}$ with $x + y = 1$ is at most $3 \cdot 7^{3+2\sharp S}$, whence there are at most $3 \cdot 7^{3+2\sharp S}$ choices for λ. Hence, there are at most $3 \cdot 7^{3+2\sharp S}$ $\mathbb{Q}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ with good reduction outside S such that the points of order 2 of E are defined over $\mathbb{Q}$.

2. $[L : \mathbb{Q}] = 2$. Let Σ be the set of prime ideals of L lying above the elements of S. The curve E is isomorphic over L to an elliptic curve in Legendre form

$$E_\lambda : \quad y^2 = x(x-1)(x-\lambda),$$

where $\lambda \in L$. Then we deduce as in case 1 that there are at most $3 \cdot 7^{4+2\sharp \Sigma}$ choices for λ. Hence, there are at most $3 \cdot 7^{4+4\sharp S}$ L-isomorphism classes of elliptic curves E over $\mathbb{Q}$ with good reduction outside S. Let $L = \mathbb{Q}(\sqrt{d})$, where d is a squarefree rational integer. Then the discriminant D_L of L is d or $4d$. On the other hand, Lemma 1 yields

$$D_L = \pm 2^\alpha 3^\beta \prod_p p^{s_p},$$

where the product is taken over all the primes $p \geq 5$, with $s_p = 0$ for p outside S, $0 \leq s_p \leq 1$ for $p \in S$ and $\alpha \leq 3$, $\beta \leq 1$. It follows that there exist $2^{4+\sharp S}$ choices for L. Furthermore, Lemma 4 implies that every L-isomorphism class of elliptic curves over $\mathbb{Q}$ is divided into at most 36 pairwise distinct $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$. Thus, we conclude that there are less than

$$108 \cdot 7^{4+4\sharp S} \cdot 2^{4+\sharp S}$$

$\mathbb{Q}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ with good reduction outside S with exactly one nonzero point of order 2 defined over $\mathbb{Q}$.

3. $[L:\mathbb{Q}] = 3$ or 6. Let $K = \mathbb{Q}(\theta)$, where θ is a root of the polynomial $x^3 + Ax + B$. By Lemma 1, the discriminant of K is

$$D_K = \pm 2^{\alpha} 3^{\beta} \prod_p p^{s_p},$$

where $\alpha = 0, 2$ or 3, $\beta = 0, 1, 3, 4$ or 5 and the product is over all primes $p \geq 5$, with $s_p = 0$ for p outside S and $0 \leq s_p \leq 2$ for $p \in S$. If $S \neq \{2,3\}$, then we denote by $P(S)$ the product of the primes of $S - \{2,3\}$ and if $S = \{2,3\}$, we put $P(S) = 1$. By Lemma 2, there are at most $24570P(S)$ cubic fields of given discriminant D_K. On the other hand, there are at most $10 \cdot 3^{\sharp S - 1}$ choices for D_K. Hence, the number of choices for K and therefore for L is

$$< 81900 \cdot 3^{\sharp S} P(S).$$

If $[L:\mathbb{Q}] = 3$, we conclude, as in the previous cases, that there are less than $3 \cdot 7^{9+6\sharp S}$ choices for the L-isomorphism class of E and Lemma 4 implies that every such class splits into 6^3 L-isomorphism classes of elliptic curves over $\mathbb{Q}$. It follows that the number of $\mathbb{Q}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ with good reduction outside S such that their 2-torsion points generate over $\mathbb{Q}$ a cubic extension is

$$< 3 \cdot 10^{15} \cdot 3^{\sharp S} \cdot 7^{6\sharp S} P(S).$$

If $[L:\mathbb{Q}] = 6$, we deduce that there are less than $3 \cdot 7^{18+12\sharp S}$ choices for the L-isomorphism class of E and Lemma 4 yields that every such class splits into 6^6 L-isomorphism classes of elliptic curves over $\mathbb{Q}$. Thus, the number of $\mathbb{Q}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ with good reduction outside S such that their 2-torsion points generates over $\mathbb{Q}$ an extension of degree 6 is

$$< 2 \cdot 10^{25} \cdot 3^{\sharp S} \cdot 7^{12\sharp S} P(S).$$

Summarizing our estimates, we deduce that the number of $\mathbb{Q}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ with good reduction outside S is

$$< 10^{11\sharp S+26} P(S).$$

4. Proof of Theorem 1. We shall follow the idea of [8, Remark 6.5, p. 265]. Let $(u,v) \in \mathbb{Z}^2$ be a solution of the Mordell equation $y^2 = x^3 + k$. We associate with this solution the elliptic curve $E(u,v)$ defined by the equation

$$Y^2 = X^3 - 3uX + 2v.$$

The discriminant of $E(u,v)$ is

$$16(4(3u)^3 - 27(2v)^2) = -2^6 3^3 k.$$

It follows that $E(u,v)$ has good reduction outside 2, 3 and the primes dividing k. Suppose now that $(w,z) \in \mathbb{Z}^2$ is another solution such that the curves $E(w,z)$ and $E(u,v)$ are isomorphic over $\mathbb{Q}$. Then there is $a \in \mathbb{Q}$ such that $u = a^4 w$ and $v = a^6 z$, whence we get

$$k = v^2 - u^3 = a^{12}(y^2 - x^3) = a^{12} k.$$

Since $a \in \mathbb{Q}$, we obtain $a = \pm 1$. So $(u,v) = (w,z)$. Hence, distinct solutions (u,v) of the Mordell equation correspond to distinct $\mathbb{Q}$-isomorphism classes of elliptic curves with good reduction outside 2, 3 and the primes dividing k. Let $\omega(k)$ be the number of prime divisors of k and $P(k)$ be the product of the prime divisors p of k with $p > 3$. If the divisors of k are among 2 and 3, we put $P(k) = 1$. Thus, Theorem 2 implies that the number of solutions $(x,y) \in \mathbb{Z}^2$ to the equation $y^2 = x^3 + k$ is $< 10^{11\omega(k)+48} P(k)$.

Acknowledgements. The author wishes to thank the referee for several helpful suggestions and comments.

References

[1] A. Brumer and J. Silverman, *The number of elliptic curves over $\mathbb{Q}$ with conductor N*, Manuscripta Math. 91 (1996), 95–102.

[2] J. H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.

[3] J. H. Evertse and J. H. Silverman, *Uniform bounds for the number of solutions to $Y^m = f(X)$*, Math. Proc. Cambridge Philos. Soc. 100 (1986), 237–248.

[4] H. Hasse, *Number Theory*, Springer, Berlin, 1980.

[5] S. Lang, *Elliptic Functions*, Addison-Wesley, 1973.

[6] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. 87 (1983), 579–585.

[7] W. M. Schmidt, *Integer points on curves of genus* 1, Compositio Math. 81 (1992), 33–59.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

Department of Mathematics
Aristotle University of Thessaloniki
54006 Thessaloniki, Greece
E-mail: poulakis@ccf.auth.gr

Received on 20.4.1998
and in revised form on 19.10.1998 (3364)